NATIONAL
CYBERWATCH
CENTER

RESOURCE GUIDE

PREPARING FOR THE COLLEGIATE CYBER DEFENSE COMPETITION (CCDC):

A GUIDE FOR NEW TEAMS AND RECOMMENDATIONS FOR EXPERIENCED PLAYERS

COMMISSIONED BY THE NATIONAL CYBERWATCH CENTER:
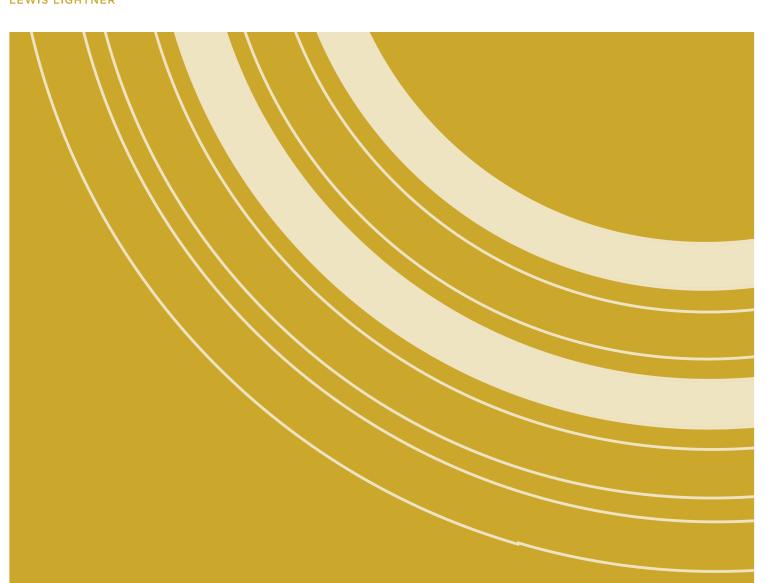
PORTIA PUSEY, ED. D.

CASEY W. O'BRIEN

LEWIS LIGHTNER

NATIONAL
CYBERWATCH
CENTER

CYBERSECURITY EDUCATION
SOLUTIONS FOR THE NATION

Many thanks to the National and Regional Collegiate Cyber Defense Competition Directors, the competitors, coaches and faculty advisors for the advice and recommendations contained in this document, including authorizing excerpts from guides and Team Packets used in this document.

Contents

Introduction

This guide was commissioned by the National CyberWatch Center. Headquartered on the Largo campus of Prince George's Community College, the National CyberWatch Center is focused on leading and supporting collaborative efforts to advance cybersecurity education and strengthen the national cybersecurity workforce. "The *CyberWatch Center's Cybersecurity Education Solutions for the Nation* project continues to help provide solutions to national cybersecurity educational challenges by leveraging its extensive network of academic institutions, government entities, and private industry partners,"

— Casey W. O'Brien, Director of the National CyberWatch Center.

Competitions are a valuable compliment to formal education because they require participants to use critical thinking and problem solving skills to complete tasks they have not seen in the classroom. Competitions can incorporate the most current vulnerabilities and attack vectors which are too new to address in college curriculum. As a national leader in creating solutions that support cybersecurity education and workforce development, the National CyberWatch Center recognizes the need grow the numbers of new players engaged in competitions. However, these new teams do not have the resources that established teams have. Experienced teams have Team Packets from past competitions. They have notebooks, and libraries of reference books. And they have mentors who can share their experience of the event. They also have the experience of competing.

In order to support new teams, the National CyberWatch Center collaborated with the National Collegiate Cyber Defense Competition and the 10 regional competitions to address the key elements needed to prepare to compete in the CCDC.

This guide will not help a team win a CCDC, but it will provide information and tips to help teams prepare. Preparation is a combination of hard work, good strategy, strong conceptual knowledge, excellent time management skills and collaborative teamwork. The CCDC is a strenuous and challenging competition and winning teams bring their own mix of strategy, teamwork, and hard work.

This guide addresses some of the frequently asked questions from new teams, "How do we get started in CCDC?" and "How do we prepare for the CCDC?" Furthermore, interviews with regional competition directors and coaches provided tips will help experienced competitors to learn practice techniques and teamwork strategies from these CCDC experts:

• Recruit and manage teams
• Build knowledge, skills and abilities
• Develop strategies
• Learn to work together

Teams should certainly not try to implement every one of the suggestions but should discuss the strengths and challenges of each of the ideas for the way their team works best.

Preparing for the CCDC also means preparing for a career in cybersecurity; this means that individuals must behave ethically and protect the institutions where they work and learn. The following messages will be repeated throughout this guide:

• Practice on machines and networks which are specifically designated for the purpose of preparing for the CCDC
• Acquire explicit permission to use the practice network and related systems
• There are sites referenced in this guide that are run by the hacker community and should be visited **AT YOUR OWN RISK**. The sites are not being operated, managed, or maintained by the National CyberWatch Center and the State, Regional, At Large and National Collegiate Cyber Defense Competitions or their affiliates; they assume no liability
• You should only practice on segregated networks with no route(s) to other networks (i.e. a closed network not connected to anything else)

Competitions

Cyber Defense Exercises and Competitions

"The goal of a Cyber Defense Competition [and Exercises] is to provide hands-on application of information assurance skills; as such, they enhance students' understanding of both theory and practice. They provide students a laboratory in which to experiment, just as in other fields of science. They fulfill the same role as capstone projects in a traditional engineering program (i.e., projects that allow students to synthesize and integrate knowledge acquired through course work and other learning experiences into a project usually conducted in a workplace). The competition combines legal, ethical, forensics, and technical components while emphasizing a team approach. Such experiential education increases the knowledge and expertise of future professionals who may be in a position to contribute to the secure design and operation of critical information and its supporting infrastructure" (from *Exploring a National Cyber Security Exercise for Colleges and Universities*, Lance J. Hoffman and Daniel Ragsdale, 2004).

History of the CCDC

On February 27 and 28, 2004, a group of educators, students, government and industry representatives gathered in San Antonio, Texas to discuss the feasibility and desirability of establishing regular cybersecurity exercises with a uniform structure for post-secondary level students. During their discussions this group suggested the goals of creating a uniform structure for cybersecurity exercises that might include the following:

1. Providing a template from which any educational institution can build a cybersecurity exercise
2. Providing enough structure to allow for competition among schools, regardless of size or resources
3. Motivating more educational institutions to offer students an opportunity to gain practical experience in information assurance

The group also identified concerns related to limiting participation to post-secondary students, creating a level playing field to eliminate possible advantages due to

National CyberWatch Center *Preparing for the Collegiate Cyber Defense Competition (CCDC): A Guide for New Teams and Recommendations for Experienced Players*

8

hardware and bandwidth differences, having a clear set of rules, implementing a fair and impartial scoring system, and addressing possible legal concerns.

In an effort to help facilitate the development of a regular, national cybersecurity exercise, the Center for Infrastructure Assurance and Security at the University of Texas at San Antonio agreed to host the first Collegiate Cyber Defense Competition (CCDC) for the Southwestern region in April of 2005.

The CCDC Competition

The mission of the CCDC is to provide institutions with an information assurance or computer security curriculum a controlled, competitive environment to assess their student's depth of understanding and operational competency in managing the challenges inherent in protecting a corporate network infrastructure and business information systems. CCDC benefits the supporting institutions of higher education by providing direct feedback for schools to exercise, reinforce, and examine their security and information technology curriculum. In higher education, formal instruction and laboratory exercises examine the abilities of a group of students to design, configure, and protect a network over the course of an entire semester; this competition extends the work of educators by testing team's technical skills under pressure. The CCDC extends the work of educators by including operational tasks for competitors to complete while teams assume administrative and protective duties for an existing "commercial" network.

The CCDC is a type of competition, also known as *Inherit and Defend*. This type of cybersecurity competition requires teams to improve the security of an existing network they have *inherited* and keep specified services running (e.g., email servers, websites, telecommunications equipment, and databases), while being attacked by hackers. In this type of competition, it is not unusual for the network and related systems to be configured atypically or incorrectly. This requires teams to use critical thinking and problem solving skills.

While similar to other cyber defense competitions in many aspects, the CCDC is unique in that it focuses on the **operational** aspects of managing and protecting an existing network infrastructure. The CCDC also tests the teams' ability to solve business challenges. This adds writing, jargon-free communication, time management, and an understanding of the importance of their work within a

company to the complexity of the CCDC. Teams are scored based on their ability to detect and respond to threats, maintain availability of existing services, respond to business requests, such as the addition or removal of additional services, and balance security needs against business needs.

CCDC events are designed to:
- Build a meaningful mechanism by which institutions of higher education may evaluate their programs
- Provide an educational venue in which students are able to apply the theory and practical skills they have learned in their course work
- Foster a spirit of teamwork, ethical behavior, and effective communication both within and across teams
- Create interest and awareness among participating institutions and students

CCDC not only benefits the students involved, but also benefits corporations as these competitors bring a more experienced skill set and proven ability to collaborate under extreme pressure to their jobs upon beginning their employment. Each CCDC experience includes a networking event to introduce industry professionals to the competitors. Networking is an additional learning experience for competitors as they interact with industry professionals to discuss many of the security and operational challenges they will soon face as they enter the job market.

CCDC Competition Overview

CCDC is one continuous contest broken into varying time periods over two-three days. The final score is cumulative for the two-three days. Each CCDC event is built around a scenario which draws attention to real-world problems. Past scenarios have included SmartGrid, Healthcare Information Technology, and disaster response. Competing teams usually receive a business communication similar to the following:

> *You have just been hired as the network and security administrators at a small company and will be taking administrative control of all information systems. You know very little about the network, what security level has been maintained, or what software has been installed (there may have even been some sabotage from disgruntled employees.) You have a limited time frame to familiarize yourself with the network and systems and to begin the security updates and patches before the Red Team starts actively attacking your company. In the midst of all the commotion, you have to keep up with the needs of the business and user demands while maintaining service level agreements for all critical Internet services. Welcome to the first day of the National Collegiate Cyber Defense Competition.*

CCDC competitions begin by asking teams to assume administrative and protective duties for an existing "commercial" network – typically a small company with 50+ users, 7-10 servers, and common Internet services such as a web server, mail server, and e-commerce site. Each team is assigned an identical set of hardware and software.

As stated before, the scores are based on a team's ability to detect and respond to threats, maintain availability of existing services, respond to business requests, and balance security needs against business needs. Throughout the competition an automated scoring engine is used to verify the functionality and availability of each team's services on a periodic basis and traffic generators continuously feed simulated user traffic into the competition network. A volunteer Red Team provides the "external threat" all Internet-based services face and allows the teams to match their defensive skills against live opponents.

While the CCDC provides a realistic IT environment, it is designed to provide scenarios and situations which push teams to address unrealistic expectations, using unfamiliar configurations and technologies, under tight time restrictions. Volatility, uncertainty, complexity and ambiguity are the hallmarks of the CCDC. However, strict attention has been paid to create a fair and even playing field:

- Each team begins with an identical set of hardware and software; they are given a small, pre-configured, operational network to secure and maintain. Teams must use the assigned hardware as they are not permitted to bring in any hardware or storage devices; nor can they access any software or tool that is not freely available on the internet. This eliminates any potential advantage for larger schools or organizations that may have better equipment or a larger budget.
- Each team is assigned their own dedicated internal network. To remove the variables associated with VPNs and propagation delay each team's network will be connected to a competition network allowing equal bandwidth and access for scoring and Red Team actions. This also allows tight control over competition traffic.
- All teams are assigned the same business objectives and technical tasks to complete. Furthermore, all teams receive the objectives and tasks at the same time during the course of the competition.
- Each team is assigned their own room during the competition. Only competition team members and White Team members will be allowed inside competition rooms to eliminate the potential influence of coaches during the competition.
- A non-biased Red Team is used which consist of volunteer, experienced Red Team security professionals who are briefed on the competition rules and restrictions. Additionally the Red Team actions are formulated so that all teams receive the same attacks.

Recruiting and Organizing

Recruiting is unique to each institution; in small schools recruiting team members can be challenging. Participation on a CCDC team requires a substantial time commitment and can be difficult for some students. Students who have a significant course load, or work full time have to be creative with their time. In order to recruit busy students, teams have to plan ways to include these students. For example, allowing the students to participate through virtual practices eliminates commuting time. It also allows students who are parents to participate from home without paying for a baby sitter. One common recommendation to recruit new members (and to keep current members happy) is to provide *free* food.

Another option is to inform potential team members of the support role they can play. Teams consist of several different types of members. There are eight *competition team members*, and an additional four alternates who may be tapped to play in a CCDC event based on team strategy or in the event a competition team member is not available for an event. However, the full roster of 12 students benefit from other students who are willing to contribute in a support role. Support ranges from setting up practice networks (real or in virtual environments) to researching and creating reference notebooks, or sharing their knowledge to prepare the team.

In general, recruiting is most effective when the faculty/school advisor or team captain visits Information Technology, Computer Science, Web Development, Security and other related classes in the beginning of the semester. These advisors and team captains are more motivated to recruit new team members than faculty who are not invested in the team. Identifying sources for team members vary by school, but some suggested sources include:

- Invite students from the IT, Networking, Computer Science, and/or Security programs
- Invite the Web Development students, with the assumption they know how to write code/script
- Develop a Computer/Security Clubs. Some schools build the team as a part of the computer/security club
- Conduct a special topics course

- Solicit recommendations from current players
- Post fliers on bulletin boards, email lists, school websites to generate interested walk-ins

Organizing the Team

> *"Make no mistake, this is a team event and the team will usually be no stronger than their weakest member. Your specific team roster need not be decided until later, but you should have all your potential team members practice working together to solve IT issues/problems/requests in a time limited fashion. During these practice sessions it may become clear who your team leaders may be[1]."*

In some cases the faculty/school advisor is the leader of the team; in other cases, the students direct the team. In general, there are two ways teams are organized and they are both equally effective: centralized, or decentralized. In the centralized model, a team captain or faculty member is responsible for all decision making. In the decentralized model, several team members and/or faculty member can be accountable for important tasks. In many cases, the organization of the team changes based on the availability and strengths of the team and the faculty/team advisor.

About CCDC Teams

All teams need a faculty/school representative. This representative does not have to be involved in all the preparation activities. However, they will need to travel with the team to all face-to-face competitions, respond to CCDC communications, and provide the competition director with team rosters and payments (if applicable). This advisor must be an official representative of the school. Furthermore, the school representative does not have to be actively involved in cybersecurity education, research or practice. Teams can find experts in the diverse topics they will need to practice among industry experts and the IT, Networking, Computer Science, Cybersecurity departments at their school.

Two weeks prior to the first CCDC event, each faculty/school representative must submit a roster of up to 12 competitors to the competition director. No changes to the team roster are permitted after the team competes in their first CCDC event.

The CCDC rules allow for a maximum of eight members to play in a CCDC event. While the faculty team representative can change the team of 8 that competes between a qualifier and a regional (or between the regional and nationals), the eight *competition team members* must come from the roster of 12. (See CCDC Rules[2] for specific details about the eligibility for CCDC team rosters.)

Team members who will not be listed on the roster, or compete in the CCDC, can support the team in several ways. It is certain that as the roster-ed team members practice setting up networks and administering systems and applications, they will encounter technical problems that they cannot resolve. Team support members can research these problems and teach the roster-ed players the solution.

Furthermore, since external storage devices and student computers are not allowed during the competition (unless otherwise told so), some competition team use a library of paper resources to serve as reference materials during the competition. In addition to published reference books, many teams create checklists, and how-to guides in notebooks. Team support members can document and research best practice and methods and organize this information into binders.

Every student has specialized talents thanks to personal interest and different life/work experiences. This specialized knowledge can benefit the competition team as they identify areas of need in their own knowledge. The support team member can provide one-on-one tutorial sessions, or teach the whole team. Teaching will strengthen the skill of the support team member as he/she responds to questions from the team. And sharing this specialized knowledge strengthens the skills and abilities of the whole team.

Another support task involves acting as a Red Team member to challenge the competition team during practice. Some students, especially those who plan to become penetration testers, would prefer to hone their offensive skills. Hardening the network and addressing Red Team attacks are important parts of the CCDC competition. Practicing with a Red Team is a good way to prepare.

Finally, support team members who would aspire to compete in the CCDC can use their role as an opportunity to learn and improve their knowledge skills and abilities. By troubleshooting, preparing resources, teaching and serving as a practice Red Team member, support team members not only strengthen the team as a whole, but build their own skillset. Support team members often earn a spot on the competition team this way.

---

1. http://www.southwestccdc.org/teamprep.html

2. http://www.nationalccdc.org/index.php/competition/competitors/rules

Organizing Tasks

Running a team involves some administrative tasks that have to be assigned in order to assure the practices take place and are productive. Support team members can perform these organizing tasks. However, since many of the tasks reinforce the leadership skills and chain of command, the team captains often are responsible for the tasks. CCDC directors have identified several tasks that can help manage a team and make constructive use of practice time. These include arranging for the practice environment, setting a schedule, identifying the practice content, assigning research projects, leading the development of a team strategy, and communicating competition rules and requirements.

Some schools have special labs for security courses, with a separate network and diagnostic and penetration testing tools. It seems like common sense, but time in this lab needs to be reserved. Teams should designate one member who will reserve this lab for practice. Other teams solicit donations and collect the hardware to create their own network. These teams must find a place to store this equipment where they can also practice. A team member should be responsible for the equipment as well as scheduling the place to practice. Finally, some teams use virtual environments to practice. Team members use their own laptops or school-provided systems to connect this environment. One team member should be responsible for the practice schedule.

No matter where teams practice it is important that the practice schedule is not only maintained, but communicated to the team. It is helpful if one team member handles the communication tasks. Team meeting reminders, changes to the schedule, practice topics, and requests for resources are all things that need to be communicated to the team. These communications should all come from the same team member.

Most teams follow a sequential order in their practices. They set up servers, address services, configure and harden, then check their work. All of these tasks may not occur in one practice session. It is advised that the activities for the subsequent practices are agreed upon before the team finishes the current practice. This enables the team members to think about, study and plan for the next practice. One individual should assume responsibility for initiating the discussion about the next practice session's task and identifying any extra resources that will be needed.

One task that can be completed outside of practice time is research. Team created notebooks are a helpful compliment to commercial reference books. While it is helpful for competition teams to do many configuration and hardening tasks without looking in a book, the pressures of competition can cause involuntary lapses in

memory. Checklists can help keep the configuring and hardening processes on task. It is also helpful to have quick reference guides for unfamiliar services and operating systems. These guides should provide instructions on how to administer a system locally and remotely, changing default credentials, security configurations, finding logs and errors. The National Security Agency has developed security configuration guides for software[3]; these can be used as a reference.

Research and practice will help a team develop a strategy for the competition. This is an important organizing task. Stated simply, strategy is a flexible plan that identifies **who** does **what**, and **when**. Strategy begins with identifying specific tasks that align with the strength of specific team members' knowledge, skills and abilities; this is the **who**. But, what differentiates each team is the relationship of the team members and the distinct variations in the knowledge, skills and abilities of each team. Every year, and perhaps every competition, as the composition of the team changes, the strategy must change too.

3. http://goo.gl/aw7sUX

What the team can accomplish depends on the skillset of the team members. The CCDC tasks stretch a team thin, and during the competition, decisions will be made based on various and often competing variables. However, prior to the competition, the team needs to discuss the strengths of the team. Who are the team members? What does he/she do best? This will determine what can be realistically accomplished within the time limit – the **when**.

The makeup of the team will also control how the team approaches the inherited systems and services they are administering. For example, based on the talents of the competition team, a strategy may be developed to switch an email server from one operating system to another, while maintaining and providing the exact same functionality. The CCDC rules state that services need to be up and accepting connections and also must be functional and serve the intended business purpose. It is helpful if one member, usually the team captain, leads the strategy discussion and develops an official strategy that will guide the team's actions during the competition.

While all these organizational tasks are important there is one overriding function that must be completed - all team members need to know the rules of the CCDC competition. All of a team's preparations can become irrelevant if they are disqualified or penalized because of a rule infraction. As a three-tier competition, the rules may be different at the qualifying, regional, and national levels. Furthermore, the rules may change annually. The rules are published in every team packet for

every competition and on the National CCDC site. It is crucial that all members read and know the rules of each competition.

Team Size

Teams can be large or small. Small teams have 8 or fewer members. Eight is the maximum number of students that compete in a given CCDC event. In this case, all team members will compete in the qualifying event, and if successful, the Region and National CCDC events. During practice, all team members rehearse their role(s) for the competition and develop skills that the team needs.

Large teams, teams with more than 8 members, can organize in several different ways. Team members can develop specialized skills based on individual interest; this provides the team some redundancy in their roster of 12 players. Team members can practice in teams of 8; this gives the competing team experience working and problem solving together. Or, all team members can all work together to practice. If all members practice together, a roster and competing team can be developed from this large pool of candidates.

Rosters

Selecting the Roster

Most CCDC Competition Directors, faculty/school advisors, and team members credit the ability of the competition team to work together and communicate well under stressful conditions as the factors that separate winning teams from the others. Teams have diverse management styles, technical skills, and strategies, but winning a CCDC event comes down to effective and efficient teamwork and leadership. This should be the first thing teams consider when picking members for the roster and competition team. Forming the roster and competition team often times depends on the size of the team.

If the team has a large pool of candidates, some schools offer tryouts, mini competitions or skills challenges to identify competition team members with a strong skillset and good collaboration skills. Other schools use a Junior Varsity (JV) to varsity system. The Varsity Team is the roster of players who will compose the competition team. The JV team practices, supports and learns as a way to earn a spot on the Varsity Team.

There are also authoritative and democratic ways of selecting a team. Some faculty/school advisors have an active role as the team organizer. As a skilled observer of the team during practice, the advisor may pick the team. At other schools, the team captain has the responsibility for choosing his/her team members for a given event. Some teams are more democratic—they hold discussions among all the potential team members and together they nominate members based on the team strategy and the needs of the team. Often times, students will eliminate themselves because they feel another team member would be a better fit for the team roster.

Roster Rules

The CCDC has several rules that govern rosters[4]:

  a) Each team must submit a roster of up to 12 competitors to the Competition Director of the first CCDC event they participate in during a given CCDC competition season. Rosters must be submitted at least two weeks prior to the start of that event. All competitors on the roster must meet all stated eligibility requirements. No changes to the team roster will be permitted after the team competes in their first CCDC event. The competition team must be chosen from

the submitted roster. A competition team is defined as the group of individuals competing in a CCDC event.

b) Each competition team may consist of up to eight (8) members chosen from the submitted roster

c) Each competition team may have no more than two (2) graduate students as team members

d) If the member of a competition team advancing to a qualifying, state, regional, or national competition is unable to attend that competition, that team may substitute another student from the roster in their place prior to the start of that competition

4. http://goo.gl/Vcblv8

Skillsets

When selecting a roster, teams should prioritize an individual's ability to work collaboratively and to communicate. There are several stories in past CCDC events where poor communication contributed to a team loss. A competitor got behind in their tasks, and was afraid to ask for help. It is important to remember that **winning and losing** never come down to the action of one individual; however, **winning** is *always* the result of teams who work well together.

If a team's pool of roster candidates is large enough, look for players who have diverse skills. For example, a team member who is strong in Windows system administration AND networking. A characteristic that is used to describe well organized teams is *redundancy*. Teams should have depth and breadth in their technical knowledge skills and abilities. Experts suggest that teams identify primary, secondary and tertiary point persons for key areas (Windows system administration, UNIX/Linux system administration, Firewall administration, etc.).

It is important that competing team member's skills overlap for several reasons: First, several competition tasks may focus on the same technical area at the same time. The competitor with one unique skill will not have enough time to do all the tasks required. Furthermore, illness, work, and academic demands can wreak havoc on a roster. It is always good to have team members who can step in should one competitor have to dropout.

There is an argument to be made for including "generalists" on your roster. A generalist understands not only **how** things are done, but **why** things are done. For example, if you understand **why** you do a task in Apache you should also know **why** it is done in Internet Information Services (IIS), and then research the specifics on **how** to accomplish the task. Understanding **how** a webpage is served will help you

diagnose **why** odd things are occurring during the competition in IIS and Apache.

Team Leader/Captain

Every team needs a leader (normally the Team Captain). The Team Captain may not necessarily have the strongest technical skills. In fact, experts advise that the team leaders should not be the competition team member with the strongest technical skills. The team leader can be pulled away from the team for an extended period of time and work on the network and systems needs to continue. Once there was a Hazmat emergency and the team captain was pulled away to be "decontaminated." The team became disorganized and unfocused until the captain returned.

Team leaders are good motivators and have solid organization and time management skills. Some teams have found Team Captains from the Psychology department. Criminal justice, Business, or Communication majors also make good captains. Since it is the role of the Team Captain to prioritize, assign and keep track of tasks, it is important that the Team Captain has the ability to stay calm under pressure. The demands of the competition network and CCDC requirements are designed to be overwhelming. The Team Captain must know the capabilities of all team members so that he/she can minimize a team member's downtime. The team captain must also maintain an awareness of the ongoing projects to avoid assigning tasks that keep another team member from completing his/her task.

Good communication skills are an imperative skill for the Team Captain. This is because he/she must communicate the progress of tasks in the process of being completed, assign help where needed, and inform the team of new tasks. The Team Captain is also the point of contact for the Gold and White teams. He/she writes the incident reports, which must be clear and detailed; and speaks with the CEO, who may be angry and/or dissatisfied with the performance of a team and its members.

The rules require a team to name a Co-Captain. The Competition Team should practice with the Co-Captain acting as the lead so they are prepared for this eventuality. The Co-Captain should have strong leadership and communication skills. It is also important that the Co-Captain and Team Captain share the same strategy. Therefore, if the Co-Captain has to step in the leadership role, the transition will be seamless—the team will continue the work assigned to them by the Team Captain and new work that is assigned will be is consistent with the team's strategy.

Essential Skills for Team Roster

The CCDC is unpredictable—teams enter with little knowledge of what hardware, operating systems or clients will require the most attention during the competition.

However, it is possible to anticipate certain variables. For example, it is certain that some version of Windows and UNIX/Linux operating systems will be deployed. Therefore, Windows and UNIX/Linux system administration experience is indispensable for a competition team. The National CCDC suggests that teams have experience with the following operating systems: Windows 2008/7, Windows 2003/2000 Server and Professional, Windows XP Professional, Windows Vista, Various BSD distributions, various Linux distributions, and Solaris. The NCCDC also lists the following applications as important to know: IIS, MySQL, BIND/MS-DNS, Sendmail/ Exchange/qmail, Apache, Samba, OpenSSL, SSH, Microsoft Office, and Active Directory. While competition creators will not limit the competition to these operating systems and applications, roster-ed team members should be sure to know how to configure the security settings and administer the applications.

When planning rosters, most teams plan for a primary, secondary and sometimes tertiary point person who can address the diverse CCDC challenges. Some of the skills, knowledge and abilities that experienced CCDC competitors, coaches and directors name as essential include:
- Common Unix Printing System (CUPS)
- Computer Forensics
- Database administration
- Directory services (e.g., Active Directory)
- Domain Name System (DNS)
- E-mail Servers (Exchange and sendmail)
- File Servers
- File Transfer Protocol (FTP) services
- Hacking Tools (Note: teams should create their own toolbox to aid in the detection of suspicious activity (e.g.., websites to use, tools to download, etc.)
- HTML
- Networking devices (to include switches, firewalls, routers)
- Samba
- Secure Shell (SSH)
- SQL
- Syslog
- Virtual Private Networking (VPN)/remote access
- Web servers (both Apache and IIS)
- Windows and UNIX/Linux system administration and hardening

Practice

Practicing for the CCDC events requires that teams develop technical skills AND collaboration skills. Learning to work well together is just as important as developing the ability to solve problems when under extreme pressure. In general, practice time should be used to create and practice a plan which distributes the workload among all the machines so that the whole team can work at the same time. "Everyone's hair should be on fire[5]."

CCDC experts have some general advice for teams relating to practice. A good rule of thumb is that teams should plan for a minimum of six months practice; in fact, experienced teams begin their planning for the next year right after the current competition ends. Teams average between 10 and 30 hours of practice a week.

Strategy to Consider
Practice until you understand what is normal: The longer you practice with an operating system, the better you will know what processes, behaviors, files, and activities are part of the actual operating system. The only way to do this is with practice installing and working with different parts of the operating system and seeing what changes, adds, deletions and executions are normal (ex. what accounts should own processes, what ports should be open, etc.)
— (Hacking Exposed Computer Forensics Blog, 2013)

During practice times, teams should set time limits. High scoring teams have good time management and get tasks done on time. Teams should practice addressing the basics. For example, strong CCDC teams have developed a good game plan during practice which will help them begin changing default passwords and move as quickly as possible to patching. It is also important to practice triage and approaching problems from diverse perspectives; not all services and hardware will be available when your team needs them. Finally, teams learn to collaborate and help one another during practice. This means that team members need to know what their job is and communicate when they need help.

5. January 28, 2013, http://blog.strategiccyber.com/2013/01/28/praise-for-ccdc/

During practices teams identify players' strengths. Practice times are when teams name the primary, secondary and tertiary point persons for the important technical areas. Most of these areas are obvious: server hardware, operating systems, networking equipment, applications, hardening systems, business injects, and communication.

One area that can be forgotten is operational security. In early competitions, teams plugged USB drives into their systems, even though this drive was found taped to the underside of the desk. Another team was able to prove a Red Team member had entered their competition room during the evening, resulting in an arrest and Red Team penalty.

Since the Red Team will be disruptive during the competition, some teams practice with a Red Team. Good sources for Red Teams include professionals who work in organizations nearby, fellow students, team members, or teams from other schools. When practicing with a Red Team, be sure to check with the system administrator so that your work does not get flagged as a violation of your school's acceptable use policy. Furthermore, remember to stay within all state and federal laws—even if practicing on your own systems within your own isolated network.

Teams should not be discouraged from participating in the CCDC or practicing even if their school does not have labs and resources. The CCDC restricts the use of tools and applications to those that are freely available. And competition teams which do not have access to security labs use their own laptops with virtual machines (VMs), or those hosted by providers (e.g., Amazon's Web Services). Virtualization has made it easier for competition teams to create practice environments even if they don't have a dedicated lab. VM's enable team members, instructors, or industry experts to build practice networks, systems, and scenarios and give team members the necessary experience installing, configuring, administering, and hardening systems.

Whether in a Lab or virtually connected, here is a good sequence for practice:
- Set up servers and systems, learn how to manage and harden them
- Practice setting up and configuring security settings on the following Windows and UNIX/Linux systems:
    - HTTP/HTTPS
    - SSH (both password and public key authentication)
    - FTP
    - RDP
    - Telnet
    - SSL
    - DNS
    - Certificates
- Work with Active Directory and apply system administration best practices:
    - Create user accounts/groups
    - Set group policies to enforce security (e.g., restricted groups, user rights assignment, file/folder permissions, etc.)
    - Once you are confident with the servers and systems, connect the servers and systems together in a network
    - Create multiple subnets
    - Assure that the systems are inter-operable between servers
- Add, configure and manage services (web, email, authentication, etc.)
- As you practice, check your work. Conduct a security analysis using a penetration testing environment like Kali Linux and/or vulnerability assessment software like Nessus.
    - Rehearse hardening your systems and network (e.g., patch and set up password policies
- Research the best methods to lock-down systems and services and study security configuration guides; including the NSA Security Guides[6].

One observation made by a Red Team alumnus was that many teams waste time because they need to consult a reference manual or notebook before completing tasks which they believed a competitor should be able to do without documentation. This Red Team alum listed the following tasks as imperative to know how to do from memory:
- Operating System User Administration: Users, Groups, Sudo, Permissions, Change Passwords
- Remote access: SSH Server, VNC/RDP, Define ACLs
- Database access control: Change passwords, investigate possible Personally Identifiable Information (PII)
- Security configurations for anticipated systems and services

It is not necessary to know everything about every system by heart. In fact, practice time is a great time to pull out your reference books and try new things. Some suggested reference books are listed in Appendix A. Furthermore, teams should create a reference notebook for a list of common tasks. When competition teams practice with unfamiliar applications and operating systems, they see patterns in how common tasks are completed. If time permits, competition teams should practice the same tasks with new applications and operating systems to identify the patterns, and develop confidence-deducing methods of completing task. These tasks should include:
- Administration: local and remote
- Change: default credentials

o Rehearse: security configuration
o Locate: application, system, and/or error logs
o Identify connections to other services or databases

6. http://goo.gl/aw7sUX

Most of the recommendations for practice are in line with what individuals do to prepare for a career in IT. However, there are some practice activities which will prepare players for the concentration of disruptive challenges players will encounter during the CCDC. For example, CCDC teams have reported that the Internet has not been available for long periods to them during the competitions.

Therefore, CCDC experts suggest that teams practice patching systems and getting services running without direct access to the Internet.

> *Look for persistence mechanisms, run strings against them, and block them.*
> — **(Strategic Cyber Blog)**

Furthermore, teams are often tempted to immediately delete shells they suspect were placed by the Red Team. A Red Team member who is also an experienced penetration tester, suggested teams study various shells to learn what information can be contained within. The shells may have information about the attack vector or its source. Use practice time to learn how a given shell (e.g., Bash) works to use it to the team's advantage.

> **Strategy to Consider**
> *Quickly deploy all solutions on one server to start gaining points and then expand the complexity of the network using different servers and several firewalls.*
> — **(Sroufe, Tate, Dantu, Celikel, 2010)**

Another good use of practice time is to learn forensic tools and techniques. CCDC veterans say that the Nmap and Nessus tools are a good start. These tools can help teams find vulnerabilities, open ports, and various other issues to be remedied. Forensics techniques that teams should practice include capturing live memory and network traffic, using Volatility to find possible malware, creating and scanning

timelines for malicious activity, and working with forensic artifacts such as prefetch and the application compatibility cache.

During the competition, teams will not have time to do all of this forensic analysis; however, the first step in fixing the problem is knowing which analysis will help identify the source of the problem. Of course, during practice, you should reinforce good habits, which include using multiple methods of forensic analysis. Use the information and techniques you learn in practice to develop a sound triage strategy that will help the captain identify what work will make the most impact and be accomplished quickly.

What to Expect

The CCDC events will challenge even the best teams. It is hard, and some would say it is not for everyone:

> "The second we got on our machines, we felt overwhelmed. Too many processes were running on our machines, we had trouble accessing our Nagios and kiosk boxes, the DNS Window's box was already not resolving requests, and none of the Linux boxes allowed us to scroll upward through our command history so typing commands was more tedious than expected. At some point, we lost control of our firewall and had to reset it. This really hurt our score right away as we weren't prepared to reset the machine or knew how to find rules that red team had placed there. By the end of the first day, our team looked pretty discouraged and morale was low." – Allyn[7]

This competitor went on to write that his team recovered, learned a lot and actually had some fun when their countermeasures against the Red Team were successful. So why should you participate? Here is what one competitor wrote:

> I competed in CCDC events for 4 years and it was some of the best education I received in college. To be successful at CCDC you have to work as a team, be able to secure systems while being probed and attacked, be able to respond to business tasks, be able to communicate with non-techies while doing it, etc... When I was going through CCDC I kept thinking "is this really what it's like"? I've been working for two years now (so clearly I don't know everything about IT or security) but I can say what I learned training for and competing in CCDC has helped me more in the real world than 90% of the stuff I learned in the classroom. Is CCDC completely realistic? Of course not, it's a COMPETITION that takes place over a limited time. They have to cram things in to make it challenging. They have to put rules in place to keep it fair for all the teams. It's supposed to be hard. It's supposed to challenge you and make you think of creative ways to secure systems and solve problems. That's the whole point. If they gave you three weeks to secure a bunch of systems and then turned the

> bad guys loose, where's the challenge in that? If you can't lock down a system after weeks of no one attacking it you should be fired[8].

Many first time competitors want to know what a CCDC event is like. Sroufe, Tate, Dantu, and Celikel[9] wrote about their experience as coaches and competition organizers in their 2010 journal article. They report a chaotic, stressful, demanding competition which challenges teams to exercise good teamwork, communicate clearly, and think creatively. Many CCDC veterans advise competitors to have confidence and, no matter what the score. Team members will have learned valuable skills that employers need. Since the CCDC is a multi-day event, competitors are fully engaged in the work of the competition by the end of the first day and the anxiety of the unknown is behind them. But to calm first day nerves, here are some tips and insights on what will happen on the first day.

What will the first day be like?

A discussion about the first day would not be complete without sage advice from CCDC Alumni. Dress well; there will be opportunities to meet potential employers every day. You should dress as if you were reporting for your first day of work; it will show you are knowledgeable about business culture. In addition to looking professional, bring extra resumes and business cards; you never know who you will meet. While these two ideas will not change the outcome of the competition, they could change your future.

Your teams' contact with the sponsors and organizers begins at the door. So, it goes without saying that teams should check-in on time. As your team checks in, all members will receive identity badges and registration materials. Teams should arrive at the competition site with all of their approved resources:

- Reference books
- Team-created manuals
- Notebooks
- Pens/highlighters
- Blank notebooks
- White boards, markers, and whatever organizational tools they have used during practice

Teams should not bring any media into the contest area including personal flash drives, CDs/DVDs, computers/laptops, external drives, networking devices, tablets, etc. The CCDC will provide teams with a limited number of storage devices for file transfer between Internet and non-Internet connected systems. Teams may bring personal MP3 players provided they are not connected to competition systems at any time. Connecting any unauthorized device to the competition network will result

7. http://www.blog.asafewebsite.com/2011/03/i-survived-ccdc.html

8. http://www.reddit.com/r/netsec/comments/17dfqf/red_teaming_a_ccdc_practice_event/

in a disqualification of that team.

After check-in, all teams are required to attend the orientation session(s) where they will be introduced to the competition directors, White - Gold - and Red Teams, Sponsors and other important individuals. The orientation session will include a review of the competition rules and the scenario.

Teams will be assigned team numbers based on a random assignment system. Then teams will be assigned competition rooms or areas based on their team number. In the room or area, teams will find hardware with various operating systems and applications installed. All rooms contain the same equipment configured in the same way. Any commercial security applications distributed for the competition will also be made available for each team. Teams should not bring any software, operating systems, or tools with them to the competition. Free operating systems, tools, and applications may be downloaded during the competition.

Some first time competitors are shocked to discover that while their systems are running and "functional" the configuration is not ideal or even standard. This means the systems will be working and will be responding to the scoring checks; however it is assured that the systems will not be "intelligently" configured. One competitor wrote that the systems were "not only configured in the worst possible configurations possible but, also have tons and tons of unneeded services and software installed as well as built in backdoors and such. Last year there was everything from netcat listeners on all the Windows machines + rootkits and task scheduled scripts to other types of malware[10]."

With this in mind, a careful observation and inventory of the provided equipment and resources is recommended. One former CCDC region director provided a piece of practical advice about the CCDC competition, "Expect shenanigans." For example in past competitions, keyboards were set to foreign languages, or incorrect cables were supplied. And it is probable that the software installed on some servers will not be current and may have known security vulnerabilities that teams will need to evaluate and address.

Once the teams have been given permission to enter their area and begin working with the equipment, their team's faculty/school advisor will not be able to enter that area. However, since some faculty/school advisors volunteer as White Team members, they may observe all other teams by systematically rotating among the various rooms.

At this point, the communication between the Blue, White, and Gold teams is restricted. Most communication will be with the Team Captain. The White Team will communicate the Gold Team requests to the Team Captain and will also convey all communication from the Blue Teams to the Gold Team using formal memoranda and various other methods (e.g., phone, email, etc.). The Team Captain may also be called away for business meetings where he/she will be given tasks that must be completed.

Throughout the competition team members will be required to break for lunch and dinner. No drinks or food are permitted in the team rooms/areas. More information about the scenario and required tasks may be presented during official meal times. Often times, the importance of the timely completion of the tasks that were assigned before meals may become apparent at this time. Many competition tasks are assigned a small piece at a time and the subsequent task depends on successfully accomplishing the prior task.

Once the first day ends, teams will have a chance to reflect and hypothesize what they can improve and accomplish the following day. Some teams consider the first day a "reality check" about what actually can be accomplished. The first night is a time where teams can adjust their strategy based on their experiences from the day plan for what they may encounter the following day.

Good to Know
Knowing what to expect can make a new player feel like a veteran. Teams may feel that they are not performing well, so CCDC alumni stress that teams should stay mentally strong and remind themselves that all teams are challenged. It is possible that even a well prepared team may go through most of the competition with only fifty percent of their services working and with limited control of the machines on their network. If new teams remember this, they will spend less time criticizing themselves and more time regrouping and problem-solving. With that in mind, some competitors have been caught off guard by lack of Internet access, surprised by equipment and web application hacks and disrupted by social engineering.

Strategy to Consider
Conquer the low hanging fruit early. For example, Windows servers can be deploy to use e-mail, POP, and DNS with the click of a few buttons and can help accumulate points early on.

9. Paul Sroufe, MS, Steve Tate, PhD., Ram Dantu, PhD, and Ebru Celikel Cankaya, PhD P. Sroufe, S. R. Tate, R. Dantu, E. Celikel. — Experiences During a Collegiate Cyber Defense Competition, Journal of Applied Security Research, Vol. 5, No. 3, 2010, pp. 382–396.

10.   http://www.reddit.com/r/netsec/comments/17dfqf/red_teaming_a_ccdc_practice_event/

The following advice and information, that CCDC alumni shared, will make new teams feel like veterans.

Access to the Internet is not guaranteed and is often filtered through a proxy—once Microsoft.com was blocked accidentally. Teams should have plans in place to harden their systems if the Internet is blocked/not working/not provided. Furthermore, team networks will not be directly connected to the Internet. This enables the White Team to monitor traffic for rule violations and inappropriate content. If Internet access is granted and available, teams will be able to route out of the central network where they can download software, patches, search engines, etc.

> **Strategy to Consider**
> *Prioritize protecting credit cards and other important data from being published on the competition team's website.*

Two overlooked vectors of attack are hardware and web applications. In one competition, a team reported they forgot that the power supply could have an IP address. In addition, the power supply had a default password that was not changed. CCDC alumni recommend that teams scan their network to assure that all connections are known. In addition, teams should familiarize themselves with web application vulnerabilities and attack vectors. Security Thread wrote on the AnandTech.com boards, *"Don't forget web applications. A lot of attacks begin with an SQL injection, or some otherwise equally bonehead coding or configuration problem on the web services. Exhaustively looking for those tends to be more time consuming than many service/network level issues, but it's still worth it."* [11]

CCDC alums also share the following information and suggestions:
- Social Engineering (SE) is part of the competition
- Be prepared to adjust your plan based on the injects
- Backup, backup, and backup again
- Pay attention to operational security: check visitor credentials, monitor your equipment, use surveillance techniques, call in Law Enforcement if necessary
- Running services earn points; the sophistication and quality of the solution is not rewarded[12].
- It is possible that your team will not be given adequate resources or information to complete your tasks. Don't be rattled—problem solve

Most importantly, understand the scoring and local rules: Qualifying events may not reflect the regional or National CCDC rules. Regional events may prioritize elements of scoring differently. Furthermore, rules may change annually. Check with your competition director to know whether these rules apply:
- Competition teams may be able to purchase equipment (computers, routers, cables) using competition points
- There will be limitations placed on your team's ability to address problems. For example, changing passwords on your systems may require a written request to the Gold Team and may be restricted to once an hour (this is unique to each region)
- Competition teams may be able to remediate some of their mistakes by spending some of their competition points

Don't Forget the Basics

In 2012, Dwayne Williams, National CCDC Director, wrote a post in the CCDC Forums entitled Don't Forget the Basics[13]. His advice was echoed by experienced CCDC White, Gold and Red Team member interviews conducted to create this resource. Many teams, especially new teams, fail to address the most fundamental methods to harden their network and systems. There are some fundamental vulnerabilities that experienced CCDC competitors and the Red Team suggest teams address early in the competition.

Address Firewall/Router vulnerabilities first. In a debrief document, the Red Team stated that one of the biggest vulnerabilities they were able to exploit was poor firewall/router rules. A threaded discussion on AnandTech Forums stressed that firewall/router rules *"need to be rock solid on inbound and outbound traffic."* One competitor described a significant delay they experienced because the router/firewall was blocking legitimate traffic from inside the network. The consequence of this problem was that the team could not update software for an inject[14].

A CCDC coach described how overzealous firewall rules kept the scorebot from checking the systems. Specific suggestions relating to routers and firewalls include knowing how to implement the Intrusion Prevention System (or related) features, disabling unnecessary ports, and using console-based password resets. Competitors should keep in mind, that they will not be able to disallow password changes on the router, switch and firewall or block IP subnets and individual addresses (unless permission has been given by the event organizers).

---

11. http://forums.anandtech.com/archive/index.php/t-2218750.html

12. P. Sroufe, S. R. Tate, R. Dantu, E. Celikel. —Experiences During a Collegiate Cyber Defense Competition, —Journal of Applied Security Research, Vol. 5, No. 3, 2010, pp. 382–396.

13. Read the post here: http://www.nationalccdc.org/blog/2012/02/20/dont-forget-the-basics/.

14. Read the threaded discussion here http://forums.anandtech.com/archive/index.php/t-2218750.html

Change passwords frequently. The Red Team will attempt to decrypt your passwords overnight. So, teams should change all the passwords to unique strong passphrases daily (at a minimum). Advice from CCDC alumni recommends that teams begin with changing the default passwords. This includes service passwords. In a threaded discussion, one Red Team member said that, *"services like SQL and various management consoles are frequently overlooked by businesses and are often "easy win". When I find a blank SA password on a SQL box that is domain joined, we usually have complete network control in under 20 minutes[15]."*

Use Hardening Guides and Templates. While teams should know the commands to secure systems as quickly as possible without having to use references, it is also important to have notes on the systems and applications teams expect to encounter. A former CCDC team captain said that he created a notebook with checklists of hardening activities that was organized alphabetically by service. Then if he froze in competition, the checklist was there to keep him on track.

Additional Advice on system hardening is included in the AnandTech Forums. One contributor wrote that *"most older systems (Windows 2003, XP, etc.) are notably stupid when it comes to baseline hardening. Run Microsoft's hardening templates that ship with domain controllers, or manually follow the Center for Internet Security (CIS) hardening guides if you are so inclined. Dumb things like LanManager hashing that is on by default in Windows environments or improper umasks in UNIX/Linux systems are where privilege escalation comes from[16]."*

Stop unnecessary services and Delete accounts that are not necessary for business functionality. Teams should monitor their systems for unnecessary services. The AnandTech threads mentioned *"be careful of unnecessary services some of the old dumb finger services that give out information, as well as the old services like rsh and rlogin."* Read the full thread here: http://forums.anandtech.com/archive/index. php/t-2218750.html

Patch and update. It is recommended that teams know out how to "sneakernet" patches/updates. In many CCDC events, the Internet connected systems are not directly connected to the competition systems.

Reinstalling or restoring images are not always the solution for remediation. In past competitions the Red Team penetrated systems early so that any images restored would include their exploit. The 2013 captain of the Red Team, David Cowen, has seven year of CCDC experience. He wrote a blog post called *NCCDC 2013 Lessons Learned.* He cautioned Blue Teams from the costly Service Level Agreement (SLA) violation penalty that comes from reinstallation. Cowen writes,

"This idea that reinstalling is the best way to recover from an intrusion is something that is not isolated to CCDC students, it's a common trend in the industry. However as a CCDC competitor, you are under a microscope with an attacker who knows you have to put that system back up as soon as possible to stop the bleeding[17]."

Finally, use logs and analysis tools to keep your team aware of service status and network traffic. These logs will also help teams to provide documentation for law enforcement, injects, and incident reports. This list has been recounted to Blue Teams at every competition. This is because teams forget the basics in the heat of the competition. Teams should practice the basics during their preparation for the CCDC events so that they become second nature.

15. http://forums.anandtech.com/archive/index.php/t-2218750.html
16. Read the full thread here: http://forums.anandtech.com/archive/index.php/t-2218750.html
17. Read his full post here: http://hackingexposedcomputerforensicsblog.blogspot.com/2013_04_01_archive.html

Scoring

At the national level, CCDC Blue Teams are scored on three main areas: Critical Services, Injects and Orange Team activity, and Red Team activity. There may be variations in scoring between the state, regional, and national CCDC events - competition teams should review the rules for each event before making any plans or decisions based on scoring.

> **Good to Know**
> *There is no requirement to maintain a "mixed" environment; however, teams will be penalized for downtime and lost functionality not OS or application choice. Teams should know how to replicate the operational capabilities/functions of the original environment including all existing files, emails, web pages, etc. within a Microsoft and a Linux/Unix environment.*

1. **Critical Services:** During each CCDC event, a set of critical services is identified that teams must manage and maintain at all times. Those services are checked for functionality and availability throughout the competition. Teams gain points each time one of the measured services is "up" or functioning properly when it is checked. If one or more services are down for an extended period of time, the team will be assessed with an Service Level Agreement (SLA) violation and point penalty. A "scoring engine" will be used during the event to perform automated service checks. For example, the scoring engine may periodically attempt to retrieve one of the required web pages from each web server, and penalties assigned if such a check fails. The required services will be fully described in the information packet given to each team at the start of the event. Teams will also be given an indication of whether the scoring engine shows their required services to be available or not.

2. **Injects and Orange Team Activity:** Injects are business tasks that teams must address, or respond to, during the competition. Injects range from the very simple (e.g., resetting a user's password), to the complex (e.g., migrating web servers from IIS to Apache with zero downtime). Many injects have a written portion (e.g., writing a report detailing actions taken by your team or the creation of a new

business policy). Injects are weighted - more complex and lengthy injects are worth more points than simple injects. The Orange Team are the "customers" of the small business. Teams earn points by providing good customer service, which might include answering questions or providing step-by-step instructions.

3. **Red Team Activity:** Teams are penalized for successful Red Team activity based on the level of access obtained. User level access costs a team fewer points than root/administrator level access which costs less than the Red Team downloading a team's entire client database with credit card numbers.

The winner of the CCDC is the team with the highest cumulative score at the end of the competition.

Critical Services

In the CCDC, teams must maintain a small business network. In the real-world, if systems are not functioning, or if data is lost, the company can lose money and customers. Therefore, the CCDC implements Service Level Agreements (SLAs) to encourage teams to maintain their required services. Blue Teams are given points for each successful service check performed. For each failed service check the team receives no points. Teams will be assessed penalties for extended outages of any critical service. For example, in the 2012 National CCDC, when a service was down continuously for 6 service checks, the team was assessed a 50 point penalty. After a service was down for 6 consecutive checks, each additional 6 unsuccessful consecutive checks cost teams an additional 50-point penalty.

The White Team may provide each Blue Team a link to a website that shows the status of each of the core services during the last status check. Additionally, teams will be notified directly when a SLA violation occurs.

> **Strategy to Consider**
> *Keep your systems up and your SLA violations to a minimum. The SLA violation you take for having your services down is the largest continual point disruption we can generate as a Red Team. Since the SLA violation grows for each period you are down, keeping you down is an important Red Team strategy.*
> — *(Hacking Exposed Computer Forensics Blog, 2013)*

Certain services are expected to be operational at all times or as specified throughout the competition. In addition to being up and accepting connections, the services must be functional and serve the intended business purpose. The scoring

engine will be checking functionality, so it's not enough to have something "listening" to a specific port. The scoring engine (or scorebot) will check to make sure a web server exists and performing the desired function. For example, the web server is providing the correct content, a mail server sends and receives mail, and the DNS server responds to queries.

The official list of required services will be provided at the start of the competition. However, here are some services that have been required at past CCDC events.

- **HTTP:** a request for a specific web page will be made. Once the request is made, the result will be stored in a file and compared to the expected result. The returned page must match the expected content for points to be awarded.
- **HTTPS:** a request for a specific page will be made. Again, the request will be made, the result stored in a file, and the result compared to the expected result. The returned page needs to match the expected file for points to be awarded.
- **SMTP:** Email will be sent and received through a valid email account via SMTP. This will simulate an employee in the field using their email. Each successful test of email functionality will be awarded points. SMTP services must be able to support either unauthenticated sessions or sessions using AUTH LOGIN (base64) at all times.
- **POP3:** a simulated user connection will be made where there user logs in using a valid userid and password and checks for mail. POP3 services must accept logins as described in the critical service description.
- **SSH:** an SSH session will be initiated to simulate a vendor account logging in on a regular basis to check error logs. Each successful login and log check will be awarded points.
- **SQL:** a SQL request will be made to the database server. The result will be stored and compared against an expected result. Each successfully served SQL request will be awarded points.
- **DNS:** DNS lookups will be performed against the DNS server. Each successfully served request will be awarded points.
- **FTP:** connections are made to the FTP server (either as anonymous or as a valid user depending on what is detailed in the critical service description) to check for the presence and availability of specific files.

Business Tasks (Injects) and Orange Team
Throughout the competition, the Blue Teams will be presented with identical injects and Orange Team tasks. Injects are business tasks teams must address, or respond to, during the competition. The tasks are authentic activities performed by an IT team at any corporation. In addition to injects, the NCCDC includes an Orange Team. This team contacts the Blue Team and challenges the members to respond

to complicated problems with people with technical support. The each Blue team is presented with identical injects and Orange Team activity. Failure to attempt to complete any task will result in a team penalty and can result in a "firing" of team members.

The Blue Teams' response to the injects and Orange Team activity earns teams points or could reduce the number of points deducted. Think of the injects and Orange Team activities as customer service—keep the CEO and customers happy (without compromising security).

Competition teams should have someone on their team who can communicate clearly and provide step-by-step instructions to difficult customers. Effective teams remember that their network is a small business and their job is to meet the business needs and provide business functionality—including customer service. Advice regarding injects includes tracking all injects as they come in then confirming that the injects are assigned, are in progress, are completed, and/or abandoned. Teams use varied methods to track the injects. They post the list on a wall, write them down on paper, or have set up websites on their networks. Use a method that works best for your team, and practice it so the team has a good way of communicating responsibilities and progress on the injects.

The challenge to successful completion of the tasks revolves around the tight deadlines. Since the challenges range in complexity, the score for each inject is weighted based upon the difficulty and time sensitivity of the tasking. At the end of the time limit provided for the inject, the performance of the Blue Team is assessed and the score is adjusted. Points are awarded based upon successful completion, or partial completion of each business task. Tasks may contain multiple parts with point values assigned to each specific part.

Some tasks may require multiple steps that are issued in multiple memos/emails etc. For example, Blue Teams may be asked to set up an Intranet DNS server and then perform a zone transfer between this new DNS server and the primary one.

Several business injects are documented on the web. These include:
- Rebrand the entire web presence with the new corporate name and logo images
- Configure SSH
- Install and configure WSUS for updates
- Implement VPN access
- Install a "live chat" function on the web page
- Write a corporate policy covering appropriate use of social networking sites
- Perform a security assessment on your own network and write a report

- Upgrade workstations to Win7
- Perform a password strength audit on your systems and write a report
- Pack up all the equipment at the end of the competition
- Install Snort in less than 2 hours
- Rehost E-Commerce site from one web server to another while maintaining service functionality
- Opening an FTP service for 2 hours given a specific user name and password
- Closing the FTP after the 2 hours is up
- Creating/enabling new user accounts
- Auditing a user's activities through system logs
- Installing new software package on CEO's desktop within 30 minutes

Addressing Injects

CCDC Injects are similar to business tasks an IT professional may receive in a corporate environment. However there are strict and challenging time limits associated with each task. Teams should decide which injects are most important and prioritize the work on the injects according to time, ability, and personnel available. Points from injects can be the deciding factor as to whether a team wins or not. Teams should follow all directions and procedures contained in the inject instruction; this attention to detail is an easy way to reduce the penalties assessed to your inject score.

Each Blue Team should use the quickest, most efficient, and secure way of addressing the injects. This solution may be less than ideal; therefore the team captains should be prepared to defend the team choices to the CEO. The team captain is the only team member who will interact with the CEO. It is especially important that the team captain stays calm even when the CEO is not.

Furthermore, the team captain should avoid technical jargon when communicating with the CEO. He/she will not be interested in a highly technical discussion—the CEO will want to know what is happening to their business. The team captain should clearly communicate what the team has done to address the injects and if something went wrong, what the team will do to mitigate against a repetition of the problem in the future. If the CEO wants to discuss a Red Team action, you should provide solutions that will minimize the impact of the Red Team's action, or your service failure, in the future.

Another possibility is that the CEO may ask for a policy change that will compromise the security of a system, or perhaps violate competition policies/rules. It is the role of the Team Captain to educate the CEO and provide concrete examples about why the CEO should consider your recommendations. You need to prove to the CEO, in non-

technical terms, how his/her decision could be costly to the business; and why your solution is cost-effective and worth the inconvenience.

The CEO will expect that all reports are well written and include a summary of important information. This will allow the CEO to can scan the document quickly and still understand 1) what you have accomplished, 2) what has not been accomplished, 3) the business impact of any inject tasks not completed; and 4) what you have planned to address what has yet to be completed.

Red Team

The Red Team's mission is to find and exploit weaknesses in each Blue Team's network; this includes systems within the Blue Team's internal and external IP address space (including systems that are not being scored). Understanding the Red Team rules, strategy, and methodologies will help Blue Teams to plan their competition strategy. For example, the Red Team is permitted limited use of Denial of Service (DoS) attacks; however use will be extremely limited. No network flooding attacks will be used. Furthermore, the Red Team will not examine/assess any of the central infrastructure items.

The CCDC is a game that is engineered in the favor of the Red Team in order to test a team's ability to work under stress. Everyone competition team is in the same position; the team that performs best ("least worse" in the words of some competitors) will win. One recommendation is to apply strategies that will hamper the Red Team's effectiveness and require them to spend more time completing their tasks[18].

> **Strategy to Consider**
> *Monitor your services' logs for errors and login events. This will help your team to detect Red Team probes and intrusions. Beyond the default information, learn how to configure logs to add additional information to capture more of what your team believes the Red Team can do.*
> — *(Hacking Exposed Computer Forensics Blog, 2013)*

It is certain that the Red Team will be disruptive. But don't be discouraged; teams are able to reduce the impact of the Red Team on their score by preparing a detailed Incident Response Report. Student teams can mitigate these penalties with effective, efficient incident reporting.

18. http://www.hackingtheuniverse.com/infosec/isnews/ccdc-tips

Scoring: Red Team

The MACCDC 2012 Team Packet describes how the Red Team actions are scored against the Blue Team. The Red Team must vary their attacks to maximize their impact on the Blue Team score. This is because the Blue Team will only incur one penalty for the same methodology used on the same target. (e.g., a buffer overflow attack that allows the Red Team to penetrate a team's system will only be scored once for that system; however, a different attack that allows the Red Team to penetrate the same system will also be scored.) Only the highest level of account access will be scored per attack (e.g., if the Red Team compromises a single user account and obtains root access in the same attack the penalty will be points for root level access and not combined points for root and user level access). Some Red Team actions are cumulative (e.g., a successful attack that yields root level access and allows the downloading of user IDs and passwords will result in an additional point penalty).

The Red Team will attack each system multiple times throughout the competition, but cannot take points for gaining admin access to a system, then come back 30 minutes later, before the teams realizes this, and take additional points for gaining admin access to the same system.

Successful Red Team actions will result in penalties to the affected team's score. Red Team scoring will vary by competition; however, the following example is from the 2012 MACCDC event:
- Obtaining root/administrator level access to a team system: **100 point penalty**
- Obtaining user level access to a team system (shell access or equivalent): **25 point penalty**
- Recovery of user IDs and passwords from a team system (encrypted or unencrypted): **50 point penalty**
- Recovery of one or more sensitive files or pieces of information from a team system (configuration files, corporate data, etc.): **25 point penalty**
- Recovery of customer credit card numbers: **50 point penalty**
- Recovery of personally identifiable customer information (name, address, and credit card number): **200 point penalty**
- Recovery of encrypted customer data or an encrypted database: **25 point penalty**

As previously written, Red Team actions are cumulative. In the example scoring above, a successful attack that yielded root level access and allowed the downloading of user IDs and passwords resulted in a 150 point penalty. Red Team actions are scored on a **per system and per method** basis. This means that a Buffer Overflow attack that allows the Red Team to penetrate a team's system will only be

scored once for that system; however, a different attack that allows the Red Team to penetrate the same system will also be scored. Only the highest level of account access will be scored per attack. So, if the Red Team compromises a single user account and obtains root access in the same attack, the penalty will be 100 points for root level access and not 125 points for root and user level access.

Red Team Activities[19]

The Red Team's methodology reflects standard penetration testing techniques. They will use reconnaissance techniques to discover and identify targets. Once a target has been identified they will look for vulnerabilities and weaknesses and attempt to penetrate targets. Once penetrated, they will establish a presence on the target. With an established presence the Red Team will use pivot attacks or other means to compromise more systems. At all points in this process they will try to escalate privileges to gain complete control of the network and related systems[20].

The Red Team has access to many open source and commercial tools. Here are some of the tools:
- Nmap/Zenmap: for basic recon and port scanning
- Nessus: for detailed vulnerability analysis
- Metasploit: penetration and pivot attacks
- Core Impact: mostly for penetration with agents for pivot attacks, but also does recon and some vulnerability analysis
- Canvas: penetration, with some recon and agents for pivot attacks
- John the Ripper: for password cracking
- Netcat: for just about everything
- Cain & Abel: for password cracking
- Prank software: http://www.rjlsoftware.com/software/entertainment/

As an opening move, one Red Team member said he/she does the following: "I use nmap across all student ranges to discover the easy exploitation opportunities as quickly as possible."[21] This opening move is only one of the many possible challenges that Blue Teams will have to overcome. Blue Teams can expect to see some of the following Red Team tactics:
- Change configuration files/settings
- Add accounts (local, administrator and domain)
- Create SSH keys for future root access
- Install malware, including keyloggers and sniffers
- Install devices that provide access including: back doors, trojaned services/executables, and rootkits
- Collect password hashes for overnight cracking
- Delete/copy database tables

19. There is much written about and by Red Team members. Several Accounts of the Red Team's experiences at the CCDC can be found here:
   • http://www.informit.com/guides/content.aspx?g=security&seqNum=292
   • http://blog.strategiccyber.com/2013/04/24/national-ccdc-red-team-fair-and-balanced/

   The NCCDC 2013 Red Team Brief can be found at http://mcaf.ee/uodvk
   AudioParasitics Episode 141 (http://mcaf.ee/gep69). Raphael Mudge shows Cobalt Strike in action and includes a walk-though of scenarios with details on how some of these Red Team activities actually occur.

20. This process is described in this blog post: http://www.hackingtheuniverse.com/infosec/isnews/ma-ccdc-09-red-cell-preparation

21. The full blog post can be found here: http://blog.strategiccyber.com/2013/04/24/national-ccdc-red-team-fair-and-balanced/

The MACCDC uses the Secret Service Incident Report (SSIR) as the required format; other regions may not have a required format. Teams should inquire about the required format of the incident reports prior to any CCDC event. If there is no required format, it is recommended that teams use the SSIR, which can be found in Appendix B.

• Kill processes
• Disable essential services
• Make services invisible to the scorebot
• Use White Team members to install malware on machines using a USB drive that autoruns when inserted
• Alter scripts written by the team to work to their favor (e.g., a script written to change the passwords of every account was used to change account passwords to ones only known by the Red Team)
• Network devices are fair game
• Hack directory services
• Download emails and read communications

Incident Response Report

In CCDC events, a thorough, well-written Incident Response report on Red Team activity can reduce a team's penalties. The report is part of the incent response process. CCDC alumni describe an eight step process for incident response which should help teams lessen the impact of the Red Team's activities.

1. Throughout the competition, teams should be gathering information. In order to determine if a system has been compromised, collect evidence from multiple sources
2. If an attack has occurred, document the business impact of the problem; the mock-CEO will want to know this.
3. Next, create hypotheses about what has been done to the system(s); verify the hypotheses with the evidence that was collected.
4. Document the team's problem solving process.
5. Decide on a plan.
6. Execute the plan.
7. Document the steps the team took to remediate the problem AND prevent a future problem of this sort.
8. Complete the incident report. If possible, the report should include the Red Team

IP address with supporting documentation, log files; packet captures which can prove that the compromise is linked to Red Team activity; etc.
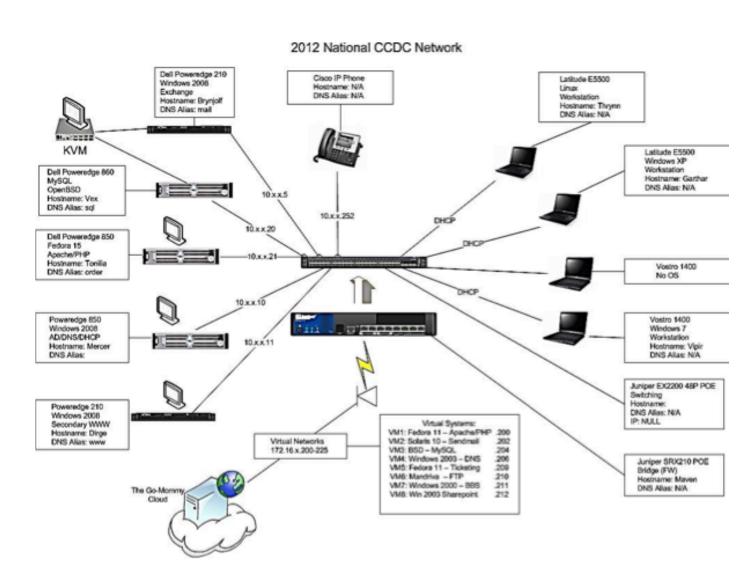
Scenarios

Competition Configurations

The scenarios are an important part of the CCDC events. The scenarios provide context for the competition. Scenarios have included inheriting and protecting a Smart Grid system, recovering from confidential data loss and the firing of an IT team, and responding as field operations units deployed to specific areas designated as local disaster aid distribution centers. The NCCDC 2012 team packet is provided in Appendix C as an example of a presentation of a scenario and related materials provided to competitors.

In the 2013 NECCDC competition, Blue Teams were told that they were hired to take over IT operations for EnV research. At the request of major stakeholders, including the Department of Energy, the previous IT team was let go after confidential and proprietary EnV research documents surfaced online. As the new IT department, Blue Teams were tasked with securing the EnV network, while maintaining business operations.[22]

The 2014 MACCDC scenario was built around disaster management. The eight Blue Teams responded as field operation units deployed to specific areas designated as local disaster aid distribution centers. The field operation teams were responsible for deploying the data systems necessary to support the disaster response activities and delivery of aid to the local site. This part of the mission involved physical layer components and establishment of connections to a higher-level management center. Once deployed, the units maintained their systems to ensure that the necessary data arrived at the Maryland Emergency Management Agency (MEMA), which was charged with distributing aid. The units were also responsible for defending their systems from a rouge disaster site. This site was actually operated by the Red Team who attempted to have aid shipments rerouted and disrupt the flow of aid. Spectators played the role of displaced persons and provided data that specified the type and quantity of aid needed.[23]

Competition Scenario

Your team, along with a new CIO, has been hired to take over IT operations for EnV research, Inc. At the request of major stake holders, including the Department of Energy, the previous IT team was let go after confidential and proprietary EnV research documents surfaced online.

As the new IT department, you will be tasked with securing the EnV network, while maintaining business operations.

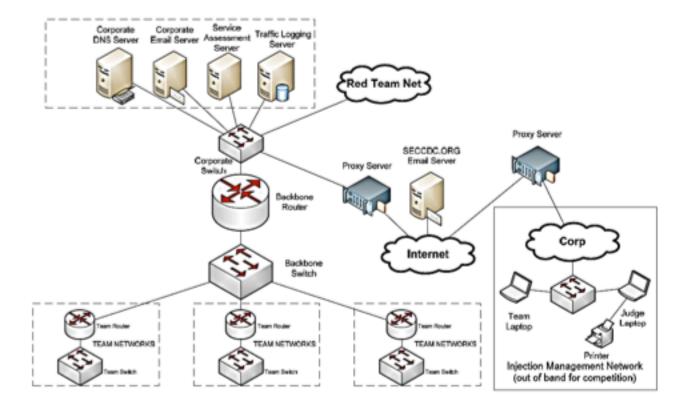Corporate Profile

EnV Research, Inc.

www.env.com

"Powering a greener world though sustainable energy solutions."

"EnV Research is a high-tech green energy startup focused on enabling renewable biofuels. Using the V372 chemical agent developed by EnV, a complex compound biofuel can be stabilized and suitable as a drop-in replacement for traditional petroleum-based fuel sources.
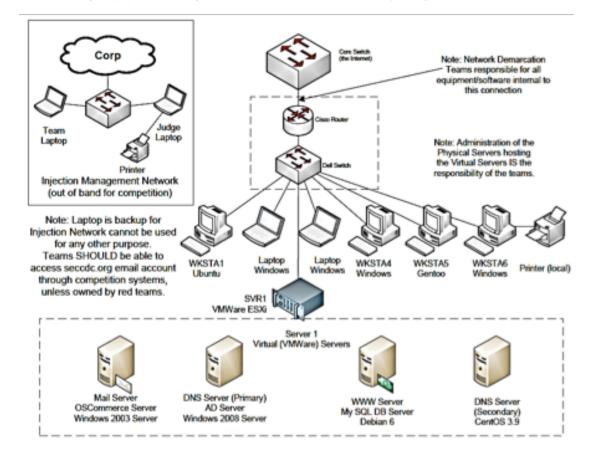
Each biofuel is different. For the V372 agent to work, the biofuel must first be tested using the EnV biofuel test kit to determine the proper levels of V372 needed. Test kits and V372 agent are purchased directly from EnV Research though its online store.

After the success of V371 which had limited availability, EnV Research commercialized V372, a next-generation agent, which quickly became used by thousands of energy companies world-wide. Today EnV is rapidly becoming one of the leading biofuel research companies in the world."

In general, CCDC events have similar network layouts. Normally, the competition networks are mostly standalone, with Internet access used primarily for obtaining patches and research. The Internet connection is either by limited external connectivity through the competition network or as a separate "outside network." The Red Team network, the White Team network, and each team network connects to a central networking device (e.g., router, firewall) that is maintained by the Operations Team.[24]
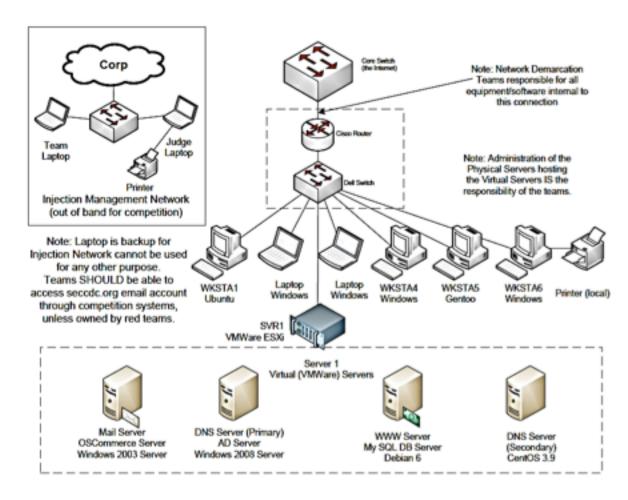
22. Northeast Collegiate Cyber-Defense Competition Team Packet (March 8-10, 2013) On0ro at the University of Maine.
    http://neccdc.net/wordpress/wp-content/uploads/2013/02/2013_NECCDC_Team_Packet.pdf

23 .http://maccdc.org/about/#sthash.YcpiuJzO.dpuf

Individual team networks are connected to the competition network through networking equipment (e.g., switch, router). The rules specify that no other

equipment may be connected to the competition network at any time (unless specifically given to the Blue Teams as part of the competition by the event organizers). Furthermore, each team is provided with an email account to send files to be worked on after hours. This email address is monitored to prevent teams from deleting it or using it for personal use.
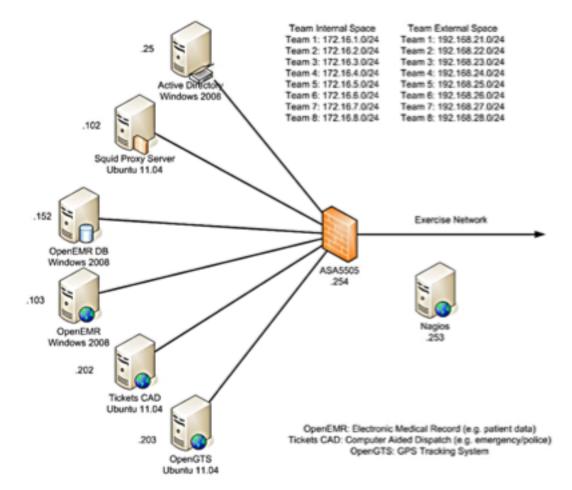

In addition to a description of the network topology, some CCDC competitions provide detailed general system information. In 2012, the MACCDC provided the following information about the systems, the roles they play and their configuration:

- Each team will be provided user-level access to a vSphere server. This server is the primary host of all your defended systems. You will connect to the vSphere server using provided PCs. Connecting information will be provided at the event.
- Team vSphere access will be limited to basic Administrator functionality. You will be able to power on/off the guest operating systems and add media (e.g., CDdrives).
- Teams will NOT be able to revert to snapshot.

24. http://www.seccdc.org/2013_docs/2013_SECCDC_TeamPacket_Final.pdf

- Teams will NOT be able to take a snapshot.
- To revert to a snapshot teams must contact Exercise Control.
- The Operations Team has access to teams' vSphere servers through an Administrator account

Post-Competition Assessment

So the competition has come to an end. The team is either still celebrating a victory or concentrating more on completing course work and perhaps enjoying a little free time. Either way the process of achieving success in the CCDC should still be present in the minds of participants and advisors. Two often understated tasks take place after the competition has concluded; post-competition debriefs and assessments. This final piece can often lead to valuable learning opportunities by giving team members a chance to analyze their individual experiences. It can also provide team advisors with information that can be used to evaluate and make improvements to programs of study. Last and definitely not least this information will lay the ground work for preparing next year's team.

A team's final score in the CCDC doesn't matter. The purpose of preparing for and playing in the competition is for players to experience activities and challenges that they might see in their future jobs. While the CCDC is an artificially generated environment, the attacks and business injects are all based on real world examples and designed by very experienced people. So, soon after the CCDC has ended it is important to schedule a debrief meeting. This will give team members an opportunity for post-competition to synthesize an understanding of their individual experience. There are several questions that can guide a post competition discussion which will provide faculty, team leaders, and future team members with the most valuable information. Some leading question may include:

- What skills were you able to apply that you learned from your course work?
- What are some examples of skills needed but no team member possessed?
- Are there skills that were needed but not presently included in your program of study?
- Describe the communications processes (or lack thereof) that occurred within the team during the competition.
- In terms of team composition in what area was the team lacking?
- Which team strategies worked and didn't work?
- Was the team effectively managed? What could have been done differently?
- Were there any obstacles that prevented the team from working together?
- Were the team member assignments relevant to the skills of those assigned?
- If you had it to do all over again how would you prepare differently for the competition?

• Reflecting on the entire CCDC process what are the most important things you learned from this experience?

Information gathered during debrief is an assessment resource available to faculty advisors as evidence for accreditation. One responsibility of schools is to prepare and conduct annual or semiannual program assessments; these processes may also be required by regional accreditation bodies. Program assessments usually involve both direct and indirect evidence of mastery of objectives. The CCDC provides a controlled environment in which to measure a student's ability to apply knowledge learned through formal education and indirectly assess programs of study. It is not likely nor possible for every objective from every program of study to be addressed at the CCDC. However it is very probable that most of the teaching that a student has experienced relevant to the competition will come into play. Faculty advisors will want to gather data during team debriefs, direct feedback of team performance, and direct observations of the team activities during the competition. Analysis of this data can provide the information necessary to indirectly measure a cross-section of students to determine their mastery of objectives. These results can then be used to reinforce and improve information technology curriculums.

Hopefully your team will lose some members every year and that's not a bad thing (after all we want them to graduate at some point). Most teams will recruit and prepare several new members for the next competition. The information gathered from the post-competition assessment process can be a valuable tool to help prepare them. No amount of learning can take the place of actual experience. The CCDC exists to provide just that. Veteran team members and experienced advisors are the key resources for new CCDC participants. **DON'T WAIT!** Start composing and preparing the team for the next competition immediately after the CCDC ends. Veteran members have the information from this year's competition fresh in their minds and perhaps even a little enthusiasm remaining to build on. You may lose that excitement over the summer so capitalize on it while it is available. By having your team ready at the beginning of the school year you'll be able to utilize the entire fall semester to prepare for the competition.

Hopefully you can see that the CCDC cycle is a continuous process of forming a team, preparing, competing, and assessing. The post-competition assessment is often the most forgotten or least emphasized. However it can be the most important for your team's success.

Appendix A: Resources

Research the CCDC. There is a lot of information available on the web regarding the CCDC. The following books are a good source of information for CCDC, but this list is not meant to be complete. Each team should research and build a library of resources that best meets their needs.

• Hacking Exposed series: www.hackingexposed.com
• Counter Hack Reloaded: www.counterhack.net/Counter_Hack/Welcome.html
• Hacking: The Art of Exploitation www.nostarch.com/hacking2.htm
• Google Hacking for Penetration Testers
• The Tao of Network Security Monitoring: www.taosecurity.com/books.html
• Nmap Network Scanning www.nmap.org/book/
• Gray Hat Hacking: The Ethical Hacker's Handbook
• Dragon Bytes: Chinese Information War Theory and Practice: Currently unavailable
• The Art of War: www.gutenberg.org/ebooks/132
• TCP/IP Illustrated, Volume I: The Protocols: www.pearsonhighered.com/bookseller/product/TCPIP-Illustrated-Volume-1-The-Protocols/9780321336316.page
• Internetworking with TCP/IP Vol. I: Principles, Protocols, and Architecture www.cs.purdue.edu/homes/comer/netbooks.html
• Modern Operating Systems: www.pearsonhighered.com/pearsonhigheredus/educator/product/products_detail.page?isbn=0136006639
• Social Engineering: The Art of Human Hacking: www.wiley.com/WileyCDA/WileyTitle/productCd-0470639539.html
• The Art of Deception: Controlling the Human Element of Security www.wiley.com/WileyCDA/WileyTitle/productCd-0471237124.html
• The Security Policy Cookbook: A Guide for IT and Security Professionals
• O'Reilly Media Select titles and access to ebooks: http://shop.oreilly.com/category/browse-subjects/security.do?sortby=publicationDate&page=3
• Cisco Press: www.ciscopress.com/store/browse/books#!?sort=Relevance
• Microsoft Press: http://shop.oreilly.com/category/microsoft-press.do
• Syngress Publishing: http://store.elsevier.com/Syngress/IMP_76

- No Starch Press: www.nostarch.com
- DHS National Checklist Program Repository: http://web.nvd.nist.gov/view/ncp/repository
- NIST Special Publications: http://csrc.nist.gov/publications/nistpubs/index.html
- Microsoft Security Guides for Security Compliance Management Toolkit Series:
  http://technet.microsoft.com/en-us/library/cc677002.aspx

Appendix B: Incident Response Report

Network Incident Report

United States Secret Service • Financial Crimes Division • Electronic Crimes Branch
Telephone: 202-406-5850   FAX: 202-406-9233   e-mail: ecb@secretservice.gov

Subject:
☐ Site under attack   ☐ Incident investigation in progress   ☐ Incident closed

What assistance do you require:
☐ Immediate call
☐ None needed at this time
☐ Follow-up on all affected sites
☐ Contact the "hacking" site(s)

Site involved *(name & acronym):*

POC for incident:
• Name / Title _____
• Organization _____
• E-mail _____ • 7 x 24 contact information _____

Alternate POC for incident:
• Name / Title _____
• Organization _____
• E-mail _____ • 7 x 24 contact information _____

Type of Incident:
☐ Malicious code: virus, Trojan horse, worm
☐ Probes/scans (non-malicious data gathering--recurring, massive, unusual)
☐ Attack (successful/unsuccessful intrusions including scanning with attack packets)
☐ Denial-of-service event
☐ High embarrassment factor
☐ Deemed significant by site

Date and time incident occurred *(specify time zone):*

A summary of what happened:

Type of service, information, or project compromised *(please provide specifics):*
☐ Sensitive unclassified such as privacy, proprietary, or source selection
   _____
☐ Other unclassified _____

Damage done:
• Numbers of systems affected_____
• Nature of loss, if any_____
• System downtime _____
• Cost of incident: ☐unknown   ☐none   ☐<$10K   ☐$10K - $50K   ☐>$50K

Name other sites contacted
Law Enforcement _____
Other: _____

UNITED STATES SECRET SERVICE   Page 1   SSF 4017 (03/2002)

Details for Malicious Code

Apparent source:
- ❑ Diskette, CD, etc.
- ❑ E-mail attachment
- ❑ Software download

Primary system or network involved:
- IP addresses or sub-net addresses _____
- OS version(s) _____
- NOS version(s) _____
- Other _____

Other affected systems or networks (IPs and OSs):

Type of malicious code (include name if known):
- ❑ Virus _____
- ❑ Trojan horse _____
- ❑ Worm _____
- ❑ Joke program _____
- ❑ Other _____

- ❑ Copy sent to
- ❑ _____
- ❑ _____
- ❑ _____

Method of Operation *(for new malicious code):*	Details:
❑ Type: macro, boot, memory resident, polymorphic, self encrypting, stealth ❑ Payload ❑ Software infected ❑ Files erased, modified, deleted, encrypted *(any special significance to these files)* ❑ Self propagating via e-mail ❑ Detectable changes ❑ Other features	

How detected:

Remediation *(what was done to return the system(s) to trusted operation):*	Details:
❑ Anti-virus product gotten, updated, or installed for automatic operation ❑ New policy instituted on attachments ❑ Firewall or routers or e-mail servers updated to detect and scan attachments	

Additional comments:

UNITED STATES SECRET SERVICE   Page 2   SSF 4017 (03/2002)

Details for Probes and Scans

Apparent source:
- IP address _____
- Host name _____
- Location of attacking host: _____
  - ❑ Domestic
  - ❑ Foreign
  - ❑ Insider

Primary system(s) / network(s) involved:
- IP addresses or sub-net addresses _____
- OS version(s) _____
- NOS version(s) _____

Other affected systems or networks (IPs and OSs):

Method of Operation:	Details:
❑ Ports probed/scanned ❑ Order of ports or IP addresses scanned ❑ Probing tool ❑ Anything that makes this probe unique	

How detected:	Details:
❑ Another site ❑ Incident response team ❑ Log files ❑ Packet sniffer ❑ Intrusion detection system ❑ Anomalous behavior ❑ User	

Log file excerpts:

Additional comments:

UNITED STATES SECRET SERVICE   Page 3   SSF 4017 (03/2002)

Details for Unauthorized Access (continued)

How detected:	Details:
❑ Another site ❑ Incident response team ❑ Log files ❑ Packet sniffer/intrusion detection software ❑ Intrusion detection software ❑ Anomalous behavior ❑ User ❑ Alarm tripped ❑ TCP Wrappers ❑ TRIPWIRED ❑ Other	

Log file excerpts:

Remediation *(what was done to return the system(s) to trusted operation):*	Details:
❑ Patches applied ❑ Scanners run ❑ Security software installed: ❑ Unneeded services and applications removed ❑ OS reloaded ❑ Restored from backup ❑ Application moved to another system ❑ Memory or disk space increased ❑ Moved behind a filtering router or firewall ❑ Hidden files detected and removed ❑ Trojan software detected and removed ❑ Left unchanged to monitor hacker ❑ Other	

Additional comments:

Details for Denial-of-Service Incident

Apparent source:

• IP address _____
• Location of host:
    ❑ Domestic
    ❑ Foreign
    ❑ Insider

Primary system(s) involved:
• IP addresses or sub-net address _____ • OS version(s) _____ • NOS version(s) _____

Other affected systems or networks (IPs and OSs):

Method of Operation:	Details:
❑ Tool used ❑ Packet flood ❑ Malicious packet ❑ IP Spoofing ❑ Ports attacked ❑ Anything that makes this event unique	

Remediation *(what was done to protect the system(s)):*	Details:
❑ Application moved to another system ❑ Memory or disk space increased ❑ Shadow server installed ❑ Moved behind a filtering router or firewall ❑ Other	

Log file excerpts:

Additional comments:

Appendix C: 2012 NCCDC

The following pages are excerpted from the 2012 NCCDC team packet. This is provided as an example of the information teams receive prior to the start of a competition.

Letter from Go-Mommy Director of IT

From: Philip Carson
To: IT Staff
Subject: Welcome

Welcome to the Go-Mommy team! We're thrilled to have you on board. As you know from your hiring briefings, we had to replace our entire group of system administrators and security personnel. And they were not happy about being fired. While everything "seems" to be working I'm quite sure we've got some major issues that need to be addressed on our network—and we're counting on you to do that for us.

You're now responsible for managing and maintaining our network. Patch and repair as you see fit, but before you go making any big changes like replacing applications or operating systems come see me for approval.

Our network really consists of two organizations. We have the main Go-Mommy network as well as our recently acquired subsidiary to maintain. That subsidiary's servers are hosted in a cloud environment off-site and we have no physical access to them—you should be able to reach them via RDP, SSH, and/or through vSphere client software. You are responsible for securing and operating that virtual environment. We have a bunch of clients running websites in that cloud and we need to protect their stuff and keep them happy. We like happy customers!

Thanks,
Philip

Competition Network Information

Here are some network addresses you will want to take note of:

     X.X.X.X – Team portal
     X.X.X.X – NTP server for official competition time
     8.8.8.8 – Google DNS
     10.X.X.1 – Default route for your team's core network
     172.16.X.1 – Default route for your team's virtual network
     X.X.X.X – Printer #1
     X.X.X.X – Printer #2
     X.X.X.X – Printer #3

Go-Mommy Network Information from the Director of IT

We are a hosting provider—the Go-Mommy network is a vital part of our business. The integrity of our network is critical. As you are all new to our organization, the outline below details what little documentation the former administrative team provided us on the inner workings of our infrastructure. While the executive staff recognizes this information is spotty at best, it should at a minimum provide your team with enough details to get you started.

Overall Network Architecture:

Network Details:
Teams are assigned IP blocks as listed below:

     Team 1 10.10.10.0 and 172.16.10.0
     Team 2 10.20.20.0 and 172.16.20.0
     Team 3 10.30.30.0 and 172.16.30.0
     Team 4 10.40.40.0 and 172.16.40.0
     Team 5 10.50.50.0 and 172.16.50.0
     Team 6 10.60.60.0 and 172.16.60.0
     Team 7 10.70.70.0 and 172.16.70.0
     Team 8 10.80.80.0 and 172.16.80.0
     Team 9 10.90.90.0 and 172.16.90.0
     Team 10 10.100.100.0 and 172.16.100.0
     Subnet mask: 255.255.255.0
     Default gateway: 10.X.X.1 or 172.16.X.1

NOTE: The .1 address belongs to the competition network and is your default gateway. Do not attempt to use the .1 address inside your team network. Do not scan, ping, probe, or mess with .1.

Passwords: The previous administrators should have set all administrative level passwords to either **"Technoviking12"**, **"password"**, or a blank password before their departure. Some equipment may still have default passwords on it.

Critical Services: In order for our business to function properly the following functionality must be available at all times and open to any IP address.

  SMTP: You must maintain ALL SMTP services on
  • 10.X.X.5
  • 172.16.X.202

  POP3: You must maintain the POP3 service on
  • go-mommy.com at 10.X.X.5

  DNS: You must maintain the DNS services on
  • 10.X.X.10 must resolve all addresses for the core and the virtual
  • 172.16.X.206

  FTP: You must maintain the FTP service on
  • 172.16.X.210

  SSH: You must maintain the SSH services on
  • 172.16.X.200
  • 172.16.X.202
  • 10.X.X.21

  HTTP: You must maintain ALL web services (and content and functionality) on
  • 10.X.X.21
  • 10.X.X.11
  • 172.16.X.200

  Telnet: You must maintain the Telnet service on
  • 172.16.X.211

  ICMP: You must allow ICMP traffic from any source to reach all systems in the virtual environment. Our clients use this to monitor the status of their systems.

  VoIP: Inside your network is a Cisco VoIP phone with an IP address of 10.X.X.252. You must allow it to communicate with the 10.120.0.X and 10.110.0.X network for your voice service to work. If you restrict the traffic to/from this phone you must

determine the ports required for VoIP communications and allow those in and out of your network.

NOTE: Go-mommy has a 99.9% uptime guarantee in place for all Platinum level clients. SLAs for Platinum customers are 6 checks.

Platinum level clients are:
  • Kwikepills
  • Jockxpress
  • Landros
  • Initech

Internally you will need to maintain:
  • File Servers
  • Client Workstations
  • Active Directory
  • Network Printing
  • Internet Access

Outbound Services:
Your user base will need unrestricted outbound access to common protocols such as HTTP, HTTPS, SSH, FTP, SFTP, POP3, DNS, update services, etc.

As our business needs change, so might the preceding list of necessary services shown above. The list provided above is merely a snapshot in time of what we currently need to properly function. Failure to provide any of these services for a prolonged amount time costs our company money and may ultimately cost you your job.

Please note that systems identified as user workstations must remain user workstations—they cannot be re-tasked, reloaded, etc unless you are instructed to do so with an inject. You will have one laptop that has no operating system on it – that system you may reload, change, or update. That laptop is yours to use as you see fit.

Networks available for internal NAT:
You may use any 10.X.X.0 network for internal NAT where the second octet matches your team network's second octet. For example Team 1 could use 10.10.20.0, Team 2 could use 10.20.90.0, Team 3 could use 10.30.20.0, and so on. Please note those networks will not be routed across the competition network.

Team Network Diagram

Dell Poweredge 210
Windows 2008
Exchange
Hostname: Brynjolf
DNS Alias: mail

Cisco IP Phone
Hostname: N/A
DNS Alias: N/A

Latitude E5500
Linux
Workstation
Hostname: Thrynn
DNS Alias: N/A

KVM

Latitude E5500
Windows XP
Workstation
Hostname: Garthar
DNS Alias: N/A

ll Poweredge 860
/SQL
enBSD
stname: Vex
IS Alias: sql

10.x.x.5

10.x.x.252

DHCP

ll Poweredge 850
dora 15
ache/PHP
stname: Tonilia
NS Alias: order

10.x.x.20

10.x.x.21

DHCP

Vostro 1400
No OS

oweredge 850
indows 2008
/DNS/DHCP
ostname: Mercer
NS Alias:

10.x.x.10

10.x.x.11

DHCP

Vostro 1400
Windows 7
Workstation
Hostname: Vipir
DNS Alias: N/A

oweredge 210
Windows 2008
econdary WWW
ostname: Dirge
NS Alias: www

Juniper EX2200 48P POE
Switching
Hostname:
DNS Alias: N/A
IP: NULL

Virtual Networks
172.16.x.200-225

Virtual Systems:
VM1: Fedora 11 – Apache/PHP   .200
VM2: Solaris 10 – Sendmail   .202
VM3: BSD – MySQL   .204
VM4: Windows 2003 – DNS   .206
VM5: Fedora 11 – Ticketing   .209
VM6: Mandriva – FTP   .210
VM7: Windows 2000 – BBS   .211
VM8: Win 2003 Sharepoint   .212

Juniper SRX210 POE
Bridge (FW)
Hostname: Maven
DNS Alias: N/A

The Go-Mommy
Cloud